Docket No. 043034-0182

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	Shigeru MARUYAMA
Title:	APPARATUS AND METHOD FOR PREVENTING UNAUTHORIZED USE OF AN INFORMATION PROCESSING DEVICE
Appl. No.:	10/804,093
Filing Date:	3/19/2003
Examiner:	Jakieda R. Jackson
Art Unit:	2626
Confirmation No.:	7905

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop APPEAL BRIEF - PATENTS
Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

Sir:

The following is the Appellants' Appeal Brief under the provisions of 37 C.F.R. 41.37.

1. Real Party in Interest

The real party in interest is NEC Corporation, which is the assignee of record.

2. Related Appeals and Interferences

None.

3. Status of Claims

The present appeal is directed to claims 1-4, 6, 7, 9-12, 14 and 15, which are the only claims pending. A copy of the presently pending claims under rejection are attached herein in the Claims Appendix (Section 9). Claims 5, 8, 13 and 16-19 were previously canceled.

4. Status of Amendments

No amendments are being filed concurrently with this Appeal Brief.

5. Summary of the Claimed Subject Matter

The present invention is directed to an information processing device having speech input and processing functions, so as to prevent unauthorized use of the information processing device. See page 1, lines 3-6 of the specification.

Independent claim 1 recites:

An unauthorized use prevention apparatus included in an information processing device, comprising:

a speech feature memory storing identifying speech feature data previously obtained from voice of an authorized user;

a password generator for generating a password which is a string of arbitrary characters;

a password notifying section for notifying a present user of the generated password;

a speech feature extractor for extracting speech feature data from voice of the present user to produce input speech feature data;

a speech feature comparator for comparing the input speech feature data to the identifying speech feature data to produce a speech feature comparison result;

a password comparator for comparing an input password obtained from the voice of the present user to the generated password to produce a password comparison result;

a controller for determining whether to inhibit the use of the information processing device, depending on the speech feature comparison result and the password comparison result; and

a database storing a plurality of entries, each of which includes address information accompanied with a password check flag,

wherein the information processing device is included in a communication device capable of voice communication, and

wherein, when a telephone dialing request operation occurs, the controller searches the database for address information related to a telephone number corresponding to the telephone dialing request operation and, when the password check flag accompanying the

address information found indicates that password check is needed, starts an unauthorized use preventing operation to prevent voice communication to be made to the telephone number corresponding to the telephone dialing request operation,

wherein, when a second telephone dialing request operation occurs, the controller searches the database for address information related to a second telephone number corresponding to the second telephone dialing request operation and, when the password check flag accompanying the address information found indicates that password check is not needed, allows operation to set up voice communication to be made to the second telephone number corresponding to the second telephone dialing request operation.

Support for "*An unauthorized use prevention apparatus included in an information processing device*" in the preamble of claim 1 may be found, for example, in Figure 1 of the drawings, portable telephone device 10. See also page 6, lines 9-15 of the specification.

Support for "*a speech feature memory storing identifying speech feature data previously obtained from voice of an authorized user*" may be found, for example, in Figure 1 of the drawings, speech feature memory 15. See also page 7, lines 24-26 of the specification.

Support for "*a password generator for generating a password which is a string of arbitrary characters*" may be found, for example, in Figure 1 of the drawings, password generator 17. See also page 8, lines 8-24 of the specification.

Support for "*a password notifying section for notifying a present user of the generated password*" may be found, for example, in Figure 1 of the drawings, display 20. See also page 10, lines 7-14 of the specification.

Support for "*a speech feature extractor for extracting speech feature data from voice of the present user to produce input speech feature data*" may be found, for example, in Figure 1 of the drawings, speech feature extractor 14. See also page 7, lines 10-17 of the specification.

Support for "*a speech feature comparator for comparing the input speech feature data to the identifying speech feature data to produce a speech feature comparison result*" may be found, for example, in Figure 1 of the drawings, speech features comparator 16. See also page 8, lines 1-3 of the specification.

Support for "*a password comparator for comparing an input password obtained from the voice of the present user to the generated password to produce a password comparison result*" may be found, for example, in Figure 1 of the drawings, password comparator 18. See also page 8, lines 8-11 of the specification.

Support for "*a controller for determining whether to inhibit the use of the information processing device, depending on the speech feature comparison result and the password comparison result*" may be found, for example, in Figure 1 of the drawings, controller 11. See also page 6, lines 11-15 and page 11, line 26 to page 14, line 2 of the specification.

Support for "*a database storing a plurality of entries, each of which includes address information accompanied with a password check flag*" may be found, for example, in Figure 1 of the drawings, memory 21. See also page 16, lines 2-16 of the specification.

Support for "*wherein the information processing device is included in a communication device capable of voice communication*" may be found, for example, in Figure 1 of the drawings, portable telephone device. See also page 6, lines 9-19 of the specification.

Support for "*wherein, when a telephone dialing request operation occurs, the controller searches the database for address information related to a telephone number corresponding to the telephone dialing request operation and, when the password check flag accompanying the address information found indicates that password check is needed, starts an unauthorized use preventing operation to prevent voice communication to be made to the telephone number corresponding to the telephone dialing request operation*" may be found, for example, page 17, lines 3-9 and 14-28, and page 18, line 23 to page 19, line 7 of the specification.

Support for "*wherein, when a second telephone dialing request operation occurs, the controller searches the database for address information related to a second telephone number corresponding to the second telephone dialing request operation and, when the password check flag accompanying the address information found indicates that password check is not needed, allows operation to set up voice communication to be made to the second telephone number corresponding to the second telephone dialing request operation*" may be found, for example, on page 17, lines 10-13 and page 18, line 23 to page 19, line 7 of the specification.

Independent claim 9 recites:

A method for preventing unauthorized use of an information processing device, comprising:

a) registering identifying speech feature data previously obtained from voice of an authorized user;

b) generating a password which is a string of arbitrary characters;

c) receiving voice of a present user sounding out the generated password;

d) comparing input speech feature data obtained from the voice of the present user to the identifying speech feature data to produce a speech feature comparison result;

e) comparing an input password obtained from the voice of the present user to the generated password to produce a password comparison result; and

f) determining whether to inhibit the use of the information processing device, depending on the speech feature comparison result and the password comparison result; and

g) storing a plurality of entries corresponding to telephone numbers, each of which includes address information accompanied with a password check flag;

when a telephone call request operation occurs to initiate a telephone call to a destination telephone number, searching the plurality of entries for address information of the destination telephone call related to the telephone call request operation; and

when the password check flag accompanying the address information found indicates that password check is needed, starting the steps b)-f),

wherein, when a second telephone dialing request operation occurs, the method comprises:

searching a database for address information related to a second telephone number corresponding to the second telephone dialing request operation and, when the password check flag accompanying the address information found in the database indicates that password check is not needed, allowing operation to set up voice communication to be made to the second telephone number corresponding to the second telephone dialing request operation.

Support for "*A method for preventing unauthorized use of an information processing device*" in the preamble of claim 9 may be found, for example, in Figures 2 and 3 of the drawings. See also page 6, lines 9-15 of the specification.

Support for "*a) registering identifying speech feature data previously obtained from voice of an authorized user*" may be found, for example, on page 11, lines 5-16 of the specification.

Support for "*b) generating a password which is a string of arbitrary characters*" may be found, for example, in Figure 2 of the drawings, "generate password 102". See also page 12, lines 2-9 of the specification.

Support for "*c) receiving voice of a present user sounding out the generated password*" may be found, for example, in Figure 2 of the drawings, "password entered using voice input 104". See also page 12, lines 8-15 of the specification.

Support for "*d) comparing input speech feature data obtained from the voice of the present user to the identifying speech feature data to produce a speech feature comparison result*" may be found, for example, in Figure 2 of the drawings, "extract input speech feature from voice input password" 105 and "input speech features matches identifying speech feature?" 106. See also page 12, lines 15-23 of the specification.

Support for "*e) comparing an input password obtained from the voice of the present user to the generated password to produce a password comparison result*" may be found, for example, in Figure 2 of the drawings, input password identical to generated password 108". See also page 12, lines 23-26 of the specification.

Support for "*f) determining whether to inhibit the use of the information processing device, depending on the speech feature comparison result and the password comparison result*" may be found, for example, in Figure 2 of the drawings, "permit the use 108" and "inhibit the use 109". See also page 13, lines 1-17 of the specification.

Support for "*g) storing a plurality of entries corresponding to telephone numbers, each of which includes address information accompanied with a password check flag*" may be found, for example, in Figure 2 of the drawings, "speech feature data stored? 101". See also page 16, lines 2-16 of the specification.

Support for "*when a telephone call request operation occurs to initiate a telephone call to a destination telephone number, searching the plurality of entries for address*

information of the destination telephone call related to the telephone call request operation" may be found, for example, page 16, lines 17-23 and page 17, lines 3-9 of the specification.

Support for "*when the password check flag accompanying the address information found indicates that password check is needed, starting the steps b)-f)*" may be found, for example, page 17, lines 3-18 of the specification.

Support for "*wherein, when a second telephone dialing request operation occurs, the method comprises: searching a database for address information related to a second telephone number corresponding to the second telephone dialing request operation and, when the password check flag accompanying the address information found in the database indicates that password check is not needed, allowing operation to set up voice communication to be made to the second telephone number corresponding to the second telephone dialing request operation*" may be found, for example, on page 17, lines 10-13 and page 18, line 23 to page 19, line 7 of the specification.

Independent claim 14 recites:

A computer readable medium storing a program, which, when executed by a computer, instructing the computer to prevent unauthorized use of an information processing device, comprising:

a) registering identifying speech feature data previously obtained from voice of an authorized user;

b) generating a password which is a string of arbitrary characters;

c) receiving voice of a present user sounding out the generated password;

d) comparing input speech feature data obtained from the voice of the present user to the identifying speech feature data to produce a speech feature comparison result;

e) comparing an input password obtained from the voice of the present user to the generated password to produce a password comparison result; and

f) determining whether to inhibit the use of the information processing device, depending on the speech feature comparison result and the password comparison result; and

g) storing a plurality of entries corresponding to telephone numbers, each of which includes address information accompanied with a password check flag;

when a telephone call request operation occurs to initiate a telephone call to a destination telephone number, searching the plurality of entries for address information of the destination telephone call related to the telephone call request operation; and

when the password check flag accompanying the address information found indicates that password check is needed, starting the steps b)-f),

wherein, when a second telephone dialing request operation occurs, the method comprises:

searching a database for address information related to a second telephone number corresponding to the second telephone dialing request operation and, when the password check flag accompanying the address information found in the database indicates that password check is not needed, allowing operation to set up voice communication to be made to the second telephone number corresponding to the second telephone dialing request operation.

Support for "*A computer readable medium storing a program, which, when executed by a computer, instructing the computer to prevent unauthorized use of an information processing device*" in the preamble of claim 14 may be found, for example, in Figures 2 and 3 of the drawings. See also page 6, lines 9-15 of the specification.

Support for "*a) registering identifying speech feature data previously obtained from voice of an authorized user*" may be found, for example, on page 11, lines 5-16 of the specification.

Support for "*b) generating a password which is a string of arbitrary characters*" may be found, for example, in Figure 2 of the drawings, "generate password 102". See also page 12, lines 2-9 of the specification.

Support for "*c) receiving voice of a present user sounding out the generated password*" may be found, for example, in Figure 2 of the drawings, "password entered using voice input 104". See also page 12, lines 8-15 of the specification.

Support for "*d) comparing input speech feature data obtained from the voice of the present user to the identifying speech feature data to produce a speech feature comparison*

result" may be found, for example, in Figure 2 of the drawings, "extract input speech feature from voice input password" 105 and "input speech features matches identifying speech feature?" 106. See also page 12, lines 15-23 of the specification.

Support for "*e) comparing an input password obtained from the voice of the present user to the generated password to produce a password comparison result*" may be found, for example, in Figure 2 of the drawings, input password identical to generated password 108". See also page 12, lines 23-26 of the specification.

Support for "*f) determining whether to inhibit the use of the information processing device, depending on the speech feature comparison result and the password comparison result*" may be found, for example, in Figure 2 of the drawings, "permit the use 108" and "inhibit the use 109". See also page 13, lines 1-17 of the specification.

Support for "*g) storing a plurality of entries corresponding to telephone numbers, each of which includes address information accompanied with a password check flag*" may be found, for example, in Figure 2 of the drawings, "speech feature data stored? 101". See also page 16, lines 2-16 of the specification.

Support for "*when a telephone call request operation occurs to initiate a telephone call to a destination telephone number, searching the plurality of entries for address information of the destination telephone call related to the telephone call request operation*" may be found, for example, page 16, lines 17-23 and page 17, lines 3-9 of the specification.

Support for "*when the password check flag accompanying the address information found indicates that password check is needed, starting the steps b)-f)*" may be found, for example, page 17, lines 3-18 of the specification.

Support for "*wherein, when a second telephone dialing request operation occurs, the method comprises: searching a database for address information related to a second telephone number corresponding to the second telephone dialing request operation and, when the password check flag accompanying the address information found in the database indicates that password check is not needed, allowing operation to set up voice communication to be made to the second telephone number corresponding to the second telephone dialing request operation*" may be found, for example, on page 17, lines 10-13 and page 18, line 23 to page 19, line 7 of the specification.

6. Grounds of Rejection to be Reviewed on Appeal

The grounds of rejection to be reviewed on appeal are: (1) whether the Examiner correctly rejected claims 1-4, 8-12 and 14-15 under 35 U.S.C. § 103(a) as being unpatentable over EP 1176493 to Pathuel in view of U.S. Patent Publication No. 2006/0188077 to Susen et al. and further in view of U.S. Patent No. 7,325,144 to Irisawa et al.; and (2) whether the Examiner correctly rejected claims 6 and 7 under 35 U.S.C. § 103(a) as being unpatentable over Pathuel in view of Susen et al. and Irisawa and further in view of U.S. Patent No. 6,904,526 to Hongwei.

7. Argument

I. Claim Rejections – Claims 1-4, 8-12 and 14-15 – Pathuel, Susen and Irisawa:

The final Office Action correctly recognizes that Pathuel and Susen et al. do not teach or suggest a controller that searches a database for address information related to a telephone number corresponding to a telephone dialing request operation, in which when a password check flag indicates that a password check is needed, starts an unauthorized use preventing operation. However, the final Office Action incorrectly asserts that Irisawa et al. teaches these features.

Irisawa describes switching between a requiring mode and a non-requiring mode of password code checking, which is enabled by an IC card with a CPU for accessing an EEPROM. Certain data regions of the EEPROM can be accessed by the IC card without password code checking, and other data regions of the EEPROM can only be accessed by the IC card with password code checking being performed. See Abstract of Irisawa.

The accessing of particular regions in an EEPROM of an IC card connected to a cellular phone in accordance with password checking or non-checking being performed based on checking flags existing or not existing in those regions of memory, is much different than allowing voice communications to a telephone number. Thus, it is submitted that one skilled in the art would not be motivated to combine Irisawa et al., which teaches the use of password checking or non-checking based on accesses to particular regions of a writable memory provided in an IC card, to telephone call access devices and methods (such as described in Susen) or computer login devices and methods (such as described in Pathuel). Note that

Irisawa is concerned about privacy issues related to personal information that may be stored in particular regions of the EEPROM of the IC card, which is not pertinent to call/no-call features based on password checking being made (or not being made), as recited in the presently pending claims.

The Advisory Action asserts that "Applicant's invention is an authorized use prevention apparatus (see preamble) and Irisawa teaches a portable information processing device that enables switching between requiring mode and non requiring mode for the checking of a password code to use the device while ensuring adequate security. The Irisawa reference was combined with the Pathuel and Susen reference to teach that password checking is nothing new/novel in the art and that the process is done simple to ensure security."

In reply, it is not the access to data stored in a memory that either does or does not require a password code that is being utilized in the present invention, but rather it is the access to be allowed to make a telephone call that either does or does not require a password code that is being utilized in the present invention. These are much different features, since data by itself is not being password protected in the present invention, but rather the ability to make a telephone call to a particular destination telephone number that is being password protected (to thereby require authorization) in the present invention.

Put in another way, in the present invention, when a user dials a desired telephone number and keys in the digits of the desired telephone number, unconditional inhibition or unconditional permission of use can be set by way of the present invention, which is recited in the "wherein" clauses at the end of each of the independent claims. Such unconditional inhibition or unconditional permission of use is not taught or suggested by Irisawa, or by the combination of Irisawa, Susen and Pauthel.

Accordingly, since one skilled in the art would not be motivated to combine the teachings of Pathuel, Susen and Irisawa in the manner as asserted in the final Office Action, and since Irisawa does not teach or suggest particular password protection features to allow a 'non-reading use' of something (e.g., the ability to make a telephone call), independent claims 1, 9 and 14 are patentable over the cited art of record.

Accordingly, independent claims 1, 9 and 14 are patentable over the cited art of record. Claims 3-4, 8, 10-12 and 15 depend either directly or indirectly from either claim 1, claim 9 or claim 14, and thus those claims are also patentable over the cited art of record.

II. Claim Rejections **– Claims 6 and 7 – Pathuel, Susen, Irisawa and Hongwei:**

Dependent claims 6 and 7 were rejected over the combination of Pathuel, Susen, Irisawa and Hongwei, whereby claims 6 and 7 depend from claim 1. The patentability of independent claim 1 has been discussed above in Section 7(I), whereby Hongwei does not rectify the deficiencies of Pathuel, Susen and Irisawa, as discussed in Section 7(I).

Thus, dependent claims 6 and 7 are patentable over the combination of Pathuel, Susen, Irisawa and Hongwei.

Conclusion

In view of above, Appellant respectfully solicits the Honorable Board of Patent Appeals and Interferences to reverse the rejections of the pending claims and pass this application on to allowance.

Respectfully submitted,

Date November 4, 2008

By _____

George C. Beck
Registration No. 38,072

Phillip J. Articola
Registration No. 38,819

Attorneys for Appellant

8. CLAIMS APPENDIX

LIST OF THE CLAIMS ON APPEAL (WITH STATUS IDENTIFIERS)

1. (Previously Presented) An unauthorized use prevention apparatus included in an information processing device, comprising:

a speech feature memory storing identifying speech feature data previously obtained from voice of an authorized user;

a password generator for generating a password which is a string of arbitrary characters;

a password notifying section for notifying a present user of the generated password;

a speech feature extractor for extracting speech feature data from voice of the present user to produce input speech feature data;

a speech feature comparator for comparing the input speech feature data to the identifying speech feature data to produce a speech feature comparison result;

a password comparator for comparing an input password obtained from the voice of the present user to the generated password to produce a password comparison result;

a controller for determining whether to inhibit the use of the information processing device, depending on the speech feature comparison result and the password comparison result; and

a database storing a plurality of entries, each of which includes address information accompanied with a password check flag,

wherein the information processing device is included in a communication device capable of voice communication, and

wherein, when a telephone dialing request operation occurs, the controller searches the database for address information related to a telephone number corresponding to the telephone dialing request operation and, when the password check flag accompanying the address information found indicates that password check is needed, starts an unauthorized use preventing operation to prevent voice communication to be made to the telephone number corresponding to the telephone dialing request operation,

wherein, when a second telephone dialing request operation occurs, the controller searches the database for address information related to a second telephone number corresponding to the second telephone dialing request operation and, when the password check flag accompanying the address information found indicates that password check is not needed, allows operation to set up voice communication to be made to the second telephone number corresponding to the second telephone dialing request operation.

2. (Original) The unauthorized use prevention apparatus according to claim 1, wherein the generated password is renewed each time the information processing device is put to use.

3. (Original) The unauthorized use prevention apparatus according to claim 1, wherein the password notifying section comprises a display section for displaying the generated password on screen so as to prompt the present user to sound out the generated password.

4. (Original) The unauthorized use prevention apparatus according to claim 1, wherein the password notifying section comprises a speech processor for sounding out the

generated password through a speaker so as to prompt the present user to sound out the generated password.

5. (Canceled).

6. (Previously Presented) The unauthorized use prevention apparatus according to claim 1, wherein the password generator generates a renewed password in response to a request operation of making a call.

7. (Previously Presented) The unauthorized use prevention apparatus according to claim 1, wherein the password generator generates a renewed password in response to a request operation of taking an incoming call.

8. (Canceled).

9. (Previously Presented) A method for preventing unauthorized use of an information processing device, comprising:

a) registering identifying speech feature data previously obtained from voice of an authorized user;

b) generating a password which is a string of arbitrary characters;

c) receiving voice of a present user sounding out the generated password;

d) comparing input speech feature data obtained from the voice of the present user to the identifying speech feature data to produce a speech feature comparison result;

e) comparing an input password obtained from the voice of the present user to the generated password to produce a password comparison result; and

f) determining whether to inhibit the use of the information processing device, depending on the speech feature comparison result and the password comparison result; and

g) storing a plurality of entries corresponding to telephone numbers, each of which includes address information accompanied with a password check flag;

when a telephone call request operation occurs to initiate a telephone call to a destination telephone number, searching the plurality of entries for address information of the destination telephone call related to the telephone call request operation; and

when the password check flag accompanying the address information found indicates that password check is needed, starting the steps b)-f),

wherein, when a second telephone dialing request operation occurs, the method comprises:

searching a database for address information related to a second telephone number corresponding to the second telephone dialing request operation and, when the password check flag accompanying the address information found in the database indicates that password check is not needed, allowing operation to set up voice communication to be made to the second telephone number corresponding to the second telephone dialing request operation.

10. (Original) The method according to claim 9, wherein the generated password is renewed each time the information processing device is put to use.

11. (Original) The method according to claim 9, wherein the generated password is displayed on a display of the information processing device so as to prompt the present user to sound out the generated password.

12. (Original) The method according to claim 9, wherein the generated password is sounded out through a speaker of the information processing device so as to prompt the present user to sound out the generated password.

13. (Canceled).

14. (Previously Presented) A computer readable medium storing a program, which, when executed by a computer, instructing the computer to prevent unauthorized use of an information processing device, comprising:

a) registering identifying speech feature data previously obtained from voice of an authorized user;

b) generating a password which is a string of arbitrary characters;

c) receiving voice of a present user sounding out the generated password;

d) comparing input speech feature data obtained from the voice of the present user to the identifying speech feature data to produce a speech feature comparison result;

e) comparing an input password obtained from the voice of the present user to the generated password to produce a password comparison result; and

f) determining whether to inhibit the use of the information processing device, depending on the speech feature comparison result and the password comparison result; and

g) storing a plurality of entries corresponding to telephone numbers, each of which includes address information accompanied with a password check flag;

when a telephone call request operation occurs to initiate a telephone call to a destination telephone number, searching the plurality of entries for address information of the destination telephone call related to the telephone call request operation; and

when the password check flag accompanying the address information found indicates that password check is needed, starting the steps b)-f),

wherein, when a second telephone dialing request operation occurs, the method comprises:

searching a database for address information related to a second telephone number corresponding to the second telephone dialing request operation and, when the password check flag accompanying the address information found in the database indicates that password check is not needed, allowing operation to set up voice communication to be made to the second telephone number corresponding to the second telephone dialing request operation.

15. (Previously Presented) The computer readable medium according to claim 14, wherein the generated password is renewed each time the information processing device is put to use.

16. – 19. (Canceled).

9. EVIDENCE APPENDIX

None.

10. RELATED PROCEEDINGS APPENDIX

None.